ORACLE

Critical Patch Update - January 2005

Description

This Critical Patch Update is a cumulative update (including all Oracle Security Alert #68 fixes) containing fixes for multiple security vulnerabilities. In addition, it also contains non-security fixes that are required (because of interdependencies) by those security fixes.

For more information about this new process, please see the Oracle Critical Patch Update Program General FAQ (MetaLink Note 290738.1).

The Critical Patch Update introduces the Risk Matrix as a method to allow customers to gauge the severity of the vulnerabilities addressed. The matrix provides the following information:

- The access required to exploit the vulnerability. If a network attack is possible, we will list the protocol used by the attack.
- The credentials and additional circumstances required to exploit the vulnerability.
- The risk of the vulnerability being exploited. This is categorized by the risk to confidentiality (e.g., privacy), integrity (e.g., information modification), and availability (e.g., service interruption). Each categorization indicates the ease with which the vulnerability can be exploited and the potential harm a successful attack can cause. The most serious vulnerabilities are Easy vulnerabilities that have a Wide impact.
- The earliest supported release indicates the first product version, that is still supported, affected by the vulnerability and the last affected patchset indicates the last patchset for each supported release that is still affected by the vulnerability. As an example:

  A customer is using Oracle Database 10*g* Release 1, version 10.1.0.2, and wishes to determine if they are affected by the DB06 vulnerability. In the Oracle Database Server Risk Matrix, the DB06 row shows '10*g*' in the Earliest Supported Release Affected column, and '10.1.0.3.1 (10*g*)' in the Last Affected Patch Set column. This means that all supported versions of 10*g* up to and including 10.1.0.3.1 are affected by the vulnerability. Therefore, this customer is affected.

- The component that contained the vulnerability is listed. In many cases, a vulnerability can be exploited solely due to the component being present on the system, even if it is not used. The component information should not be used to determine if a system is vulnerable to a given attack. This information is provided to aid customer testing.
- Finally, we will indicate if recommended workarounds are available, and if so, what they are. Workarounds that may adversely affect the operation of other Oracle products are not provided.

MetaLink Note 293956.1 defines the terms used in the Risk Matrix.

Please note: Oracle has analyzed each potential vulnerability separately for risk of exploit and impact of

exploit. Oracle has performed no analysis on the likelihood and impact of blended attacks (i.e. the exploitation of multiple vulnerabilities combined in a single attack).

Policy Statement on Information Provided in Critical Patch Updates and Security Alerts

Oracle Corporation conducts an analysis of each security vulnerability addressed by a Critical Patch Update (CPU) or a Security Alert. The results of the security analysis are reflected in the severity of the CPU or Security Alert and the associated documentation describing, for example, the type of vulnerability, the conditions required to exploit it and the result of a successful exploit. Oracle provides this information, in part, so that customers may conduct their own risk analysis based on the particulars of their product usage.

As a matter of policy, Oracle will not provide additional information about the specifics of vulnerabilities beyond what is provided in the CPU or Security Alert notification, the pre-installation notes, the readme files, and FAQs. Oracle does not provide advance notification on CPU or Security Alerts to individual customers. Finally, Oracle does not develop or distribute active exploit code, nor "proof-of-concept" code, for vulnerabilities in our products.

Critical Patch Update Availability for De-Supported Versions

Critical Patch Updates are available for customers who have purchased Extended Maintenance Support (EMS). De-support Notices indicate whether EMS is available for a particular release and platform, as well as the specific period during which EMS will be available.

Customers with valid licenses for product versions covered by Extended Support (ES) are entitled to download existing fixes; however, new issues that may arise from the application of patches are not covered under ES. Therefore, ES customers should have comprehensive plans to enable backing out any patch application.

Oracle will not provide Critical Patch Updates for product versions which are no longer covered under the Extended Maintenance Support plan. We recommend that customers upgrade to the latest supported version of Oracle products in order to obtain Critical Patch Updates.

Please review the "Extended Support" section within the Technical Support Policies for further guidelines regarding ES & EMS.

Supported Products Affected

The following supported product releases and versions are affected by this Critical Patch Update:

- Oracle Database 10*g* Release 1, versions 10.1.0.2, 10.1.0.3 and 10.1.0.3.1 (10.1.0.3.1 is supported for Oracle Application Server only)
- Oracle9*i* Database Server Release 2, versions 9.2.0.4, 9.2.0.5 and 9.2.0.6
- Oracle9*i* Database Server Release 1, versions 9.0.1.4, 9.0.1.5 and 9.0.1.5 FIPS (all of which are supported for Oracle Application Server only)
- Oracle8*i* Database Server Release 3, version 8.1.7.4
- Oracle8 Database Release 8.0.6, version 8.0.6.3 (supported for E-Business Suite only)

- Oracle Application Server 10*g* Release 2 (10.1.2)
- Oracle Application Server 10*g* (9.0.4), versions 9.0.4.0 and 9.0.4.1
- Oracle9*i* Application Server Release 2, versions 9.0.2.3 and 9.0.3.1
- Oracle9*i* Application Server Release 1, version 1.0.2.2
- Oracle Collaboration Suite Release 2, version 9.0.4.2
- Oracle E-Business Suite and Applications Release 11i (11.5)
- Oracle E-Business Suite and Applications Release 11.0

The new database vulnerabilities addressed by this Critical Patch Update do not affect Oracle Database Client-only installations (installations that do not have the Oracle Database Server installed). Since this Critical Patch Update includes all fixes from Security Alert 68, the client fixes in this Critical Patch Update are the same as Security Alert 68. If Security Alert 68 has not been applied to Client-only installations, Security Alert 68 or this Critical Patch Update must be installed on those installations in order to eliminate the security vulnerabilities described by Security Alert 68.

Unsupported products, releases and versions have not been tested for the presence of these vulnerabilities, nor patched, in accordance with section 4.3.3.3 of the Software Error Correction Support Policy (MetaLink Note 209768.1). However, earlier patchset levels of the affected releases are most likely also affected by these vulnerabilities.

Oracle Database Server

Oracle Database Server Risk Matrix

Please refer to Appendix A - Oracle Database Server Risk Matrix.

Oracle Database Patch Availability

Please see the Pre-Installation Note for the Oracle Database Server, MetaLink Note 293737.1.

Oracle Enterprise Manager Grid Control

There are no new fixes for Oracle Enterprise Manager Grid Control in this Critical Patch Update. However, since this Critical Patch Update includes all fixes in *Security Alert 68*, the Oracle Enterprise Manager fixes in this Critical Patch Update are the same as *Security Alert 68*.

Oracle Enterprise Manager Patch Availability

Please see the Pre-Installation Note for the Oracle Enterprise Manager Grid Control, MetaLink Note 295108.1.

Oracle Application Server

Oracle Application Server Risk Matrix

Please refer to Appendix B - Oracle Application Server Risk Matrix.

Oracle Application Server Patch Availability

Please see the Pre-Installation Note for the Oracle Application Server, MetaLink Note 293738.1.

Oracle Collaboration Suite

Oracle Collaboration Suite Risk Matrix

Please refer to Appendix C - Oracle Collaboration Suite Risk Matrix.

Oracle Collaboration Suite Patch Availability

Please see the Pre-Installation Note for the Oracle Collaboration Suite, MetaLink Note 293740.1.

Oracle E-Business and Applications

This Critical Patch Update contains security fixes for Oracle8 Database Release 8.0.6 version 8.0.6.3 released in revision 3 of Alert 68 on December 27th, 2004. All E-business customers must apply these patches.

Oracle E-Business Risk Matrix

Please refer to Appendix D - Oracle E-Business Risk Matrix.

Oracle E-Business Patch Availability

Please see the Pre-Installation Note for the Oracle E-Business Suite, MetaLink Note 293741.1.

References

- Critical Patch Update – January 2005 FAQ, MetaLink Note 293955.1
- Oracle Critical Patch Update Program General FAQ, MetaLink Note 290738.1
- Oracle Critical Patch Update Documentation Tree, MetaLink Note 294914.1
- Security Alerts and Critical Patch Updates- Frequently Asked Questions, MetaLink Note 237007.1

Credits

The following people discovered and brought security vulnerabilities addressed by this Critical Patch Update to Oracle's attention: Pete Finnigan, Alexander Kornbrust of Red Database Security, Stephen Kost of Integrigy, David Litchfield of NGSS Limited.

Modification History

18-JAN-05: Initial release, version 1

15-MAR-05: This revision of the advisory documents two Application Server vulnerabilities that are already mentioned in the Application Server Pre-Installation Note. They have been added to the Application Server Risk Matrix for completeness.

Appendix A

Oracle Database Server Risk Matrix
Critical Patch Update – January 2005

				RISK								
				Confidentiality		Integrity		Availability				
Vuln#	*Component*	*Access Required (Protocol)*	*Authorization Needed (Package or Privilege Required)*	*Ease*	*Impact*	*Ease*	*Impact*	*Ease*	*Impact*	*Earliest Supported Release Affected*	Last Affected Patch set (per Supported Release)	*Work-around*
DB01	Networking	SQL(Oracle Net)	Database (create database link)	Difficult	Wide	Difficult	Wide	Easy	Wide	8	8.0.6.3(8), 8.1.7.4 (8*i*), 9.0.1.4(9*i*)	---
DB02	LOB Access	SQL(Oracle Net)	Database (read on database directory object)	Easy	Wide	---	---	---	---	8*i*	8.1.7.4(8*i*), 9.0.1.5 (9*i*)	---
DB03	Spatial	SQL(Oracle Net)	Database (execute on mdsys.md2)	Difficult	Wide	Difficult	Wide	Easy	Wide	8*i*	8.1.7.4(8*i*), 9.0.1.5 (9*i*), 9.2.0.5(9*i*R2), 10.1.0.3.1(10*g*)	---
DB04	UTL_FILE	SQL(Oracle Net)	Database (read on database directory object)	---	---	Easy	Limited	---	---	9*i*R2	9.2.0.5(9*i*R2)	---
DB05	Diagnostic	SQL(Oracle Net)	Database	Difficult	Wide	Difficult	Wide	Easy	Wide	8*i*	8.1.7.4(8*i*), 9.0.1.5 (9*i*), 9.2.0.4(9*i*R2)	---
DB06	XDB	SQL(Oracle Net)	Database (execute on xdb.dbms_xdb)	Difficult	Limited	Difficult	Limited	---	---	10*g*	10.1.0.3.1(10*g*)	---
DB07	XDB	SQL(Oracle Net)	Database (execute on xdb.dbms_xdbz0)	Difficult	Limited	Difficult	Limited	---	---	9*i*R2	9.2.0.5(9*i*R2), 10.1.0.3.1(10*g*)	---
DB08	XDB	SQL(Oracle Net)	Database (execute on xdb.dbms_xdbz0)	Difficult	Limited	Difficult	Limited	---	---	10*g*	10.1.0.3.1(10*g*)	---
DB09	Expression Filter	SQL(Oracle Net)	Database (execute on exfsys.dbms_expfil)	Difficult	Limited	Difficult	Limited	---	---	10*g*	10.1.0.3.1(10*g*)	---
DB10	Log Miner	SQL(Oracle Net)	Database (execute on dbms_logmnr)	Difficult	Limited	Difficult	Limited	---	---	9*i*R2	9.2.0.5(9*i*R2)	---
DB11	OLAP	SQL(Oracle Net)	Database (execute on olapsys)	Difficult	Limited	Difficult	Limited	---	---	9*i*R2	9.2.0.5(9*i*R2), 10.1.0.3.1(10*g*)	---
DB12	Data Mining	SQL(Oracle Net)	Database (execute on dmsys.dmp_sys)	Difficult	Limited	Difficult	Limited	---	---	10*g*	10.1.0.3.1(10*g*)	---

DB13	Advanced Queuing	SQL(Oracle Net)	Database (execute on dbms_transform_eximp)	Difficult	Wide	Difficult	Wide	---	---	10*g*	10.1.0.3.1(10*g*)	---
DB14	Change Data Capture	SQL(Oracle Net)	Database (execute on dbms_cdc_dputil)	Difficult	Wide	Difficult	Wide	---	---	10*g*	10.1.0.3.1(10*g*)	---
DB15	Change Data Capture	SQL(Oracle Net)	Database (execute on dbms_cdc_impdp)	Difficult	Wide	Difficult	Wide	---	---	10*g*	10.1.0.3.1(10*g*)	---
DB16	Database Core	SQL(Oracle Net)	Database	Easy	Wide	Easy	Wide	---	---	10*g*	10.1.0.3.1(10*g*)	---
DB17	Oracle HTTP Server	Network (HTTP)	Database (execute on owa_opt_lock)	Difficult	Limited	Difficult	Limited	---	---	8*i*	8.1.7.4(8*i*), 9.0.1.5 (9*i*), 9.2.0.6(9*i*R2)	---

- If further credentials or specific configurations are required to exploit the vulnerability, they will be listed in the **Required Conditions, Oracle Database Vulnerabilities** section of this document.
- If a workaround is indicated, the **Workarounds, Oracle Database Vulnerabilities** section of this document describes a workaround for the ***Vuln#*** given above.

Required Conditions, Oracle Database Vulnerabilities

These are additional conditions that are required in order to exploit the given vulnerability.

- *DB01* The ability to CREATE DATABASE LINK is necessary.
- *DB02, DB04* Read permission on a database directory object is needed.
- *DB03* The ability to execute procedures in the mdsys.md2 package is necessary.
- *DB06* The ability to execute procedures in the xdb.dbms_xdb package is necessary.
- *DB07, DB08* The ability to execute procedures in the xdb.dbms_xdbz0 package is necessary.
- *DB09* The ability to execute procedures in the exfsys.dbms_expfil package is necessary.
- *DB10* The ability to execute procedures in the dbms_logmnr package is necessary.
- *DB11* The ability to execute procedures in the olapsys package is necessary.
- *DB12* The ability to execute procedures in the dmsys.dmp_sys package is necessary.
- *DB13* The ability to execute procedures in the dbms_transform_eximp package is necessary.
- *DB14* The ability to execute procedures in the dbms_cdc_dputil package is necessary.
- *DB15* The ability to execute procedures in the dbms_cdc_impdp package is necessary.
- DB17 The ability to execute procedures in the owa_opt_lock package is necessary.

Workarounds, Oracle Database Vulnerabilities

There are no recommended workarounds for the Oracle Database vulnerabilities described in the Oracle Database Risk Matrix.

Appendix B

Oracle Application Server Risk Matrix
Critical Patch Update – January 2005

				RISK								
				Confidentiality		Integrity		Availability				
Vuln#	***Component***	***Access Required (Protocol)***	***Authorization Needed (Package or Privilege Required)***	***Ease***	***Impact***	***Ease***	***Impact***	***Ease***	***Impact***	***Earliest Supported Release Affected***	***Last Affected Patch set***	***Work-around***
AS01	Report Server	Network (HTTP)	None	Easy	Wide	Easy	Wide	---	---	1.0.2.2	1.0.2.2	Yes
AS02	Forms	Network (TCP)	None	---	---	---	---	Easy	Limited	1.0.2.2	1.0.2.2	---
AS03	mod_plsql	Network (HTTP)	Database (execute on owa_opt_lock)	Difficult	Limited	Difficult	Limited	---	---	1.0.2.2	9.0.4.1	---
AS04	Designer	None (image viewing)	None	Difficult	Wide	Difficult	Wide	Difficult	Wide	6i	r9.0.2.9 v9.0.2.96.6i, 10g (9.0.4) r9.0.4.5 v9.0.4.5.6i	---
AS05	Jinitiator	Network	None	Difficult	Wide	Difficult	Wide	Easy	Wide	1.1.8	1.1.8.23, 1.3.1.14	---

- If further credentials or specific configurations are required to exploit the vulnerability, they will be listed in the **Required Conditions, Oracle Application Server Vulnerabilities** section of this document.
- If a workaround is indicated, the **Workarounds, Oracle Application Server Vulnerabilities** section of this document describes a workaround for the ***Vuln#*** given above.

Required Conditions, Oracle Application Server Vulnerabilities

No further conditions are required in order to exploit the listed vulnerabilities.

Workarounds, Oracle Application Server Vulnerabilities

- *Vulnerability AS01*

  Please consult MetaLink notes 133957.1 and 119825.1.

Appendix C

Oracle Collaboration Suite Risk Matrix
Critical Patch Update – January 2005

				RISK								
				Confidentiality		Integrity		Availability				
Vuln#	***Component***	***Access Required (Protocol)***	***Authorization Needed (Package or Privilege Required)***	***Ease***	***Impact***	***Ease***	***Impact***	***Ease***	***Impact***	***Earliest Supported Patch set Affected***	***Last Affected Patch set***	***Work-around***
OCS01	Calendar	None (image viewing)	None	Difficult	Wide	Difficult	Wide	Difficult	Wide	9.0.4.2	9.0.4.2	---

- If further credentials or specific configurations are required to exploit the vulnerability, they will be listed in the **Required Conditions, Oracle Collaboration Suite Vulnerabilities** section of this document.
- If a workaround is indicated, the **Workarounds, Oracle Collaboration Suite Vulnerabilities** section of this document describes a workaround for the ***Vuln#*** given above.

Required Conditions, Oracle Collaboration Suite Vulnerabilities

These are additional conditions that are required in order to exploit the given vulnerability.

- *OCS01* A user must be forced to view an image of unknown provenance in order to exploit this vulnerability.

Workarounds, Oracle Collaboration Suite Vulnerabilities

There are no recommended workarounds for the Oracle Collaboration Suite vulnerabilities described in the Oracle Collaboration Suite Risk Matrix.

Appendix D

Oracle E-Business Suite Risk Matrix
Critical Patch Update – January 2005

			RISK								
			Confidentiality		Integrity		Availability				
Vuln#	***Access Required (Protocol)***	***Authorization Needed (Package or Privilege Required)***	***Ease***	***Impact***	***Ease***	***Impact***	***Ease***	***Impact***	***Earliest Supported Release Affected***	***Last Affected Patch set***	***Work-around***
APPS01	Network (HTTP)	Valid Session	Difficult	Wide	Difficult	Wide	---	---	11.5.2	11.5.9	---
APPS02	Network (HTTP)	None	Easy	Wide	Easy	Wide	---	---	11.0	11.5.7 and HRMS Family Pack B	---

- If further credentials or specific configurations are required to exploit the vulnerability, they will be listed in the **Required Conditions, Oracle E-Business Suite Vulnerabilities** section of this document.
- If a workaround is indicated, the **Workarounds, Oracle E-Business Suite Vulnerabilities** section of this document describes a workaround for the ***Vuln#*** given above.

Required Conditions, Oracle E-Business Suite Vulnerabilities

No additional conditions are required in order to exploit the listed vulnerabilities. An installed version of Oracle E-Business Suite and a connected session are sufficient.

Workarounds, Oracle E-Business Suite Vulnerabilities

There are no recommended workarounds for the Oracle E-Business Suite vulnerabilities described in the Oracle E-Business Suite Risk Matrix.